(Safety Device for Overall Protection of Objects with Electronic Components)

Description

Felix Huber, Ernst Messerschmid, and Wolfgang Schäfer

It is known that electrical components can be controlled remotely by radio signals. A typical application is an electronic alarm system and/or drive lock of a vehicle, which the user activates or deactivates with a transmitter. In this case, it does not matter whether the transmitter radiates directly (e.g., through infrared transmission) or public radio serves or telephone networks are connected in between. However, if anti-theft protection is implemented in such a way that the object to be protected can be reactivated by disconnecting or bridging the protection device, then the protection is practically useless.

Typical characteristics and problems of such protection will be explained with the example of a vehicle. In principle, such a protection can be used for all objects with an electronic component. This can include, among other things: radio telephone ("handies"), (Euro-)Check and money cards, credit cards, telephone cards, keys for electronic lock systems, mobile electronic devices such as cassette recorders, CD players, clocks, computers, etc.

It is known that vehicles with mechanical and/or electric anti-theft protection devices can be reactivated by disassembly or bridging. This applies especially to expensive vehicles, where the entire vehicle can simply be transported by organized bands and worked on at a safe place. It is also known that vehicles with an electronic drive lock, often part of the motor control, can only be reactivated at great expense and with special knowledge. Often, reactivation is possible only with an original key and/or by involving a contract workshop.

Since with a stolen original key the vehicle can be made ready to drive immediately, a change from simple vehicle theft to theft by personal threat is being observed. Deactivation by a small hand transmitter a few hundred meters away could be conceived, but this brings the danger that the victim himself is placed in danger if the culprit becomes aware of the existence of the transmitter.

In order to make certain that the proper owner is protected, concepts have already been thought up in which the vehicle regularly receives radio signals for release of the electronics and is deactivated if these signals are absent. In a stolen vehicle, these signals can then be turned of intentionally, so that the vehicle can no longer be operated. This, however, has the disadvantage that when a radio gap appears, which is repeatedly the case with mobile telephones, further driving is no longer possible. In addition, a gapless coverage of the radio range must also be provided in other countries, since a temporary turning off of the protection during a stay abroad again makes the protection absurd. Such protection, however, means a strong restriction for legal users and therefore cannot be put on the market.

It is also known that there are devices in which a circuit in the vehicle can be activated that deactivates the ignition electronics. Such systems can be realized through a telephone connection that the user activates by dialing a particular number assigned to the vehicle receiver. Here too, global accessibility of the vehicle must be considered. These systems, however, could be circumvented by removing the receiver from the vehicle or by correspondingly shielding it from receiving signals, so that a blocking of the ignition electronics no longer occurs.

For universal protection, therefore, the system must be constructed in such a way that reactivation cannot take place through the user himself, for otherwise the information necessary for this could be obtained by force. Also, deactivation of the system must be able to take place at any time after the theft. This deactivation can also be performed by third parties, so that a threat to or even killing of the owner does not help. For a thief, therefore, stealing such an object has no value, since within a few hours it will no longer have its desired functionality.

Method of operation

The invention avoids the disadvantages mentioned above by irreversibly deactivating and/or erasing at least one of the components 5,6,7,8 (Figure 1) and/or information within at least one of these components that are essential for operation of the vehicle, so that disassembly or bridging of the components concerned has no effect, since there is no access to the acquisition of functioning replacement parts. These components can include, e.g., the motor electronics 6, the steering column lock 7, the door lock 8, and/or the key 5.

In order to achieve worldwide protection, the radio signal 9,14 is preferably radiated by a low-orbiting satellite and/or a space station 1, both with high inclination–in order to achieve global coverage. In this case, it is not necessary to fly in a 90° polar orbit, since the transmitter 2 has a certain side width 19 and can cover the inhabited parts of the world already with a 50° inclination because of the rotation of the earth (Figure 2). In the non-covered regions, 17,18, at the poles, this use is of no interest, because there are no consumers there. With today's usual radio density and restrictions on transmitter power, a space station 1 comes into consideration preferably, since they can be kept at a maximum orbiting altitude of up to 400 km for a long period of time, in order to generate the required field strength. Control of the transmitter 2 can take place through radio or another communications medium, e.g., by calling an emergency center 3, which takes over the corresponding activation 20 of the transmitter 2.

In case of a theft of the vehicle 4, with a key 5 or forced taking of the key 5, the legitimate owner of the vehicle calls a service number by telephone or transmits in some other way information about the theft. After checking his authenticity, e.g., by giving a password in order to prevent malicious deactivation, the identification number of the stolen unit is sent by one or more ground stations 3 to the transmitter 2 in orbit. This identification (ID) number is preferably assigned unambiguously worldwide for every received and/or group of receivers 5,6,7,8, and it can be stored in a database, for example. The transmitter 2 now transmits this ID periodically, preferably worldwide, so that over the course o time the signal 9,14 can be received over the entire face of the earth 16.

The theft protection 6,7,8 in the vehicle is erased when the indispensable important information in the signal 9 and/or disturbed components is/are recognized by the on-board electronics, the key, an/or the lock, without which operation of the vehicle is no longer possible. The receiver or the decoder logic 9 and the safety-relevant components 10 preferably form a unit 21 (e.g., microprocessor with its own internal memory) so that the data traffic 11 of the electronics is "monitored" and can possibly be manipulated, so that deactivation is no longer possible.

In addition, for deactivation the vehicle 4 can also send signals back to make localization possible more easily; this is not absolutely necessary for protection of the vehicle, however. The system can also be constructed in such a way that only the legitimate owner can trigger this signal, so that an undesired permanent localization of the vehicle is impossible.

The deactivated components can be later identified as stolen by checking the serial number and/or the disturbed data. For this, a contract workshop can use a corresponding diagnostic device, with which the data from the components 5,6,7,8 can be read. False alarms and intentional deactivations are excluded, and the signal 9,14 can be provided with check sums to permit transmission and/or authenticity errors to be detected.

For safety reasons, in a vehicle that is moving, a regulated slow disconnection is preferably performed, so that the danger of an accident is avoided. This can occur in such a way that, for example, the vehicle can no longer be accelerated, and a stop is achieved by slowing down gradually. Then the motor can be turned off. In this case, it is irrelevant whether the deactivation takes place immediately or only after a time, after which the theft signal is turned off. For the potential thief, use of such a vehicle is uninteresting, since the vehicle can stop and become unusable after the theft.

It is also possible to place the receiver 4 not in the vehicle itself, but in the key 5 (distributed security). Modern drive locks preferably use no mechanical locks, but exchange keyed codes 12 between the key and the vehicle, which block the vehicle. In the case of a deactivation by a radio signal 9,14, it is therefore sufficient that at least one of the components 5,6,7,8 contain the turn-off code. At the next attempt to start the vehicle 4, the information through the data exchange 15 spreads preferable through all components, which now deactivate themselves as described above.

This data exchange can likewise not be stopped, e.g., by involving synthetic information, since signaling takes place in the absence of the correct data 12. These date 12 are generated anew when any contact is made with components 5,6,7,8, and they can only be generated and decoded by them, since the components are identified with each other at the time of manufacture (one-time coding principle).

A "repair" of the vehicle is thus (preferably) possible thereafter only by exchanging all deactivated components 5,6,7,8 at the same time. A contract workshop can determine at the time the new components are sold, which naturally involves the return of at least one of the deactivated components 5,6,7,8, whether a theft signal 9,14 was responsible for the deactivation or therefore the thief caused the vehicle 4 to stop in attempting to reactivate it. An excuse that the components were disturbed during an accident and therefore could not be presented cannot be made for the reason that an accident in which all electronic modules 6,7,8 and all keys 5 were disturbed cannot happen. Even surrendering an unauthorized key 5 that has not received a deactivation signal 14 is of no use, since in this case, the read-out of the ID and an identification with the database would immediately indicate a theft.

Distributed security also increased the reliability of the system, since vehicles are turned off under certain circumstances in areas where receiving the radio signal 9,14 is not always possible (deep garages, etc.) or the receiver is intentionally shielded. It should not happen for the legitimate user that the device is deactivated falsely through bad reception conditions. A receiver 13 integrated into the key holder is normally has good reception conditions sufficiently often and one can check regularly that the theft radio service 14 is received without errors. If this is not the case, then the receiver in question goes into a metastable state. On the next attempt to start the vehicle, the components check with each other by a comparison 15 of their data, whether at least one of the components was able to receive a signal 9,14 within the permitted time period. If so, then the system is reactivated completely. If not, then the user is signaled that radio contact must be made possible within a certain time period, since otherwise the electronics will be deactivated. If a thief omits this radio contact in a stolen vehicle, then the electronics are likewise deactivated, so that in this case the vehicle 4 remains useless to the thief.

Since the receiver can be greatly miniaturized, this system is also very well suited for devices that must make radio contact in any case, such as,

e.g., radio telephones 21 (Figure 3). The receiver in this case can be included in the chip card 22 and/or the telephone 21. If one of the devices receives a deactivation signal 23,24, at the time of the next use, when the card 22 must be inserted into the telephone 21, the chip card 22 is deactivated by the data exchange 26 between the components, whereby the telephone can still send out signals 25 even after a deactivation, so that localization is possible.

In principle, the receiver can also be built into the newest generation of check cards 27, so that here a protection of E.C. cards, credit cards, and telephone cards becomes possible. A card that receives a deactivation signal, 28,29 (this can also derive from the automatic device 30 itself) can detect likewlise erase its internal memory. At the next attempt to use the card, a money device 30 can detect this and take corresponding further steps, e.g. recording the person on video, reporting the site to the motion detector, locking the doors, etc.